Amendments to the Specification

Please replace the paragraph beginning on page 4, line 23 and ending on page 5, line 10 with the following replacement paragraph reflecting the amendments made therein:

At the sending correspondent 12, there is provided an IPSec security module 34 to implement security on the IP packet. The IPsec module 34 includes a packet interceptor 36 to intercept PPP datagrams and to decapsulate the PPP datagrams to retrieve the encapsulated IP packets. The packet interceptor 36 may be a software module such as a driver included in a kernel of the operating system in the computer readable medium of the system, placed below the PPP layer of a network stack. The IPsec module 34 determines the type of security to apply to the IP packets by referencing a security policy manager 38. The sending correspondent 12 determines what policy is appropriate for each IP packet, depending on various selectors (for example, destination IP address or transport layer ports), by looking in the security policy manager 38, which indicates the relevant policy for any particular packet. The packet either requires IPsec processing of some sort, in which case it is passed to an IPsec processing module 40 for processing; or it does not, in which case it is simply passed along for normal IP processing. The IPsec processing module 40 performs packet-per packet processing by examining the packets in order to select and apply cryptographic transformations on the IP packets as known the art. In instances where processing is not required, the IP packets may be dropped or the IP packets proceed up or down the protocol stack 18. Outbound packets are checked against the security policy manager 38 to see what kind (if any) of IPsec processing to apply, while inbound packets are checked against the security policy manager 38 to see what kind of IPsec service should be present in those IP packets.

BEST AVAILABLE COPY